STATE OF ALABAMA

Information Technology Standard

Standard 640-02S1: Remote Access Controls

1. INTRODUCTION:

The increasing mobility of State employees and contractors has made remote access to State network resources vital to conducting State business. This standard refines and expands State IT Policy 620-01: Network Access and other relevant policies and standards to address remote access (i.e., any access to the State network through a non-State controlled network, device, or medium).

2. OBJECTIVE:

Ensure remote access technologies are deployed in a manner that ensures State systems maintain acceptable levels of security and service.

3. SCOPE:

These requirements apply to all users (State employees, contractors, vendors, and business partners) who remotely access any State of Alabama information system resources, other than public web servers or systems specifically designed for public access, and to all personnel responsible for the administration of remote access services.

4. REQUIREMENTS:

The following requirements, based the recommendations of the National Institute of Standards and Technology (NIST) and the SANS (SysAdmin, Audit, Network, Security) Institute, shall apply to remote access connections to State information system resources.

4.1 MANAGEMENT CONTROLS

Access to the State network resources from remote locations (including homes, hotel rooms, wireless devices and off- site offices) is not automatically granted to users in conjunction with network or system access.

State employees and authorized third parties (consultants, vendors, etc.) may utilize remote access capabilities only with written approval of the IT Manager. Managers shall document access request-approval procedures.

Remote access to systems containing confidential or sensitive data requires the written approval of the system and/or data owner, and shall comply with the specific requirements of the data owner or of the data type (e.g., Personally Identifiable Information; see applicable State Standard).

Revoke remote access authorization when necessary for reasons including, but not limited to, changes in employment, contract termination, non-compliance with security policies, request by the system/data owner, or negative impact on overall network performance attributable to remote access communications. Review remote access authorizations at least quarterly.

4.2 ADMINISTRATIVE CONTROLS

The preferred method of remote access to State network resources is through a centrally managed Virtual Private Network (VPN) connection that provides encryption and secure authentication in accordance with State VPN standards.

Do not divulge details or instructions regarding remote access, including external network access points or dial-up numbers, unless the requester has been verified as authorized to connect to the State network as an external user.

All hosts, including privately owned personal computers, connecting remotely to State networks shall have up-to-date and properly configured anti-virus software and current operating system service pack and patch level. Hosts may be scanned to ensure compliance with State standards, and users may be denied remote access if their host system presents an unacceptable risk to State networks.

Place dial-in users under the same access policy as those connecting via VPN by placing the remote access server either in the DMZ or within a screened subnet where the VPN gateway resides.

Secure remote access shall be strictly controlled. Where possible, control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

With the exception of web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any State system or network anonymously (for example, by using “guest” user IDs).

Terminate remote access accounts in accordance with State Access Management Standards.

Systems accepting remote connections from public network connected users (users connected through phone modems, Internet Service Providers, cable modems, etc.) must temporarily terminate the connection and lock out the user ID following a series of three unsuccessful attempts to log-in.

Systems accepting remote connections from public network connected users (users connected through phone modems, Internet Service Providers, cable modems, etc.) must apply a time-out feature that terminates all sessions after no more than 30 minutes of inactivity.

Routers for dedicated ISDN lines configured for access to the State network must meet minimum authentication requirements of CHAP.

Dual-homing is not permitted.

4.3 MONITORING

Monitor remote access usage to ensure compliance with security policies.

Monitor remote access usage, and report to IT Managers when remote access communications is causing a negative impact on network performance.

5. DEFINITIONS:

CHAP: Challenge Handshake Authentication Protocol; an authentication method that uses a one-way hashing function.

DUAL HOMING: Network topology in which a device is connected to the network by way of two independent access points (e.g., wired and wireless).

ISDN: Integrated Services Digital Network, a circuit-switched telephone network system that allows digital transmission of voice and data over ordinary telephone copper wires.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-02: Remote Access

6.2 RELATED DOCUMENTS

Information Technology Policy 620-01: Network Access

Information Technology Standard 620-01S1: Access Management

Information Technology Standard 640-02S2: Virtual Private Networks

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	2/16/2007	